Vie privée, cybermarketing et cryptographie

Dinant, Jean-Marc

Published in:
Ubiquité

Publication date:
1999

Vie privée, cybermarketing et cryptographie

Par Jean-Marc DINANT[1]

Résumé

Si certaines caractéristiques du réseau Internet ont frappé les esprits juridiques (dématérialisation de l'information, temps réel, abolition des frontières), une caractéristique technique du réseau le rend préoccupant par rapport à la protection des données à caractère personnel. Contrairement à l'ordinateur personnel d'antan doté de périphériques transparents (écran/imprimante), le cyber ordinateur d'aujourd'hui est équipé d'un modem ou d'une carte réseau qui ne laisse rien transparaître de l'information reçue par le réseau ou communiquée à celui-ci. Par ailleurs, l'utilisateur néophyte n'a que peu de contrôle sur les programmes qui fonctionnent réellement sur son ordinateur. De nombreux programmes s'exécutent en effet à son insu dès le démarrage de sa machine et peuvent accéder directement au réseau, sans laisser de traces.

Ces dernières années, les firmes de marketing se sont littéralement ruées sur le réseau Internet car cette caractéristique technique d'invisibilité et d'opacité permet le profilage invisible et individuel de chaque internaute en particulier, en temps réel et au delà des frontières. Nous tenterons dans un premier temps de donner un bref aperçu des méthodes utilisées par les firmes de cybermarketing.

Pour contrer cette technologie Internet, aujourd'hui synonyme d'espionnage domestique, systématique et mercantile du citoyen ravalé au rang de consommateur, trois solutions techniques peuvent être envisagées. La première consiste à créer une contre technologie. La deuxième consiste à utiliser des solutions de chiffrement. La dernière consiste à adapter les technologies actuelles aux exigences de la protection de la vie privée. Dans un deuxième temps, nous nous proposerons de décrire brièvement ces trois types de solutions et d'apprécier leur pertinence.

Les méthodes modernes de cybermarketing

Bien souvent les défenseurs de la "privacy" peuvent apparaître comme des paranoïaques de l'informatique et des empêcheurs de ficher en rond, confondant les rumeurs d'un académique " techniquement possible " avec la constatation d'un " effectivement réalisé ". Aussi tenons à souligner que ce qui suit n'est pas l'œuvre d'une imagination fertile mais repose sur des bases solides : un rapport[2] réalisé en 1998 pour le compte du groupe 29[3] complété par une expérimentation personnelle qui a permis de mettre techniquement en évidence les mécanismes décrits dans ce rapport.

En simplifiant[4], l'on pourrait dire que *grâce aux mécanismes invisibles*[5] qui ont été intégrés et activés par défaut dans les navigateurs courants depuis plusieurs années, plusieurs millions d'internautes européens sont

---

[1] Courriel : jmdinant@fundp.ac.be. Jean-Marc DINANT est licencié, maître et doctorand de l'Institut d'Informatique à Namur. Actuellement chargé de recherche au CRID (vie privée et commerce électronique) il travaille aussi comme expert auprès de la Commission belge de protection des données et au sein de l'Internet Task Force du Groupe 29.

[2] Serge Gauthronet, " Les services en ligne et la protection des données, annexe au rapport annuel 1998 du groupe de travail établi par la directive 95/46 ", Commission européenne, 1998 : http://europa.eu.int/comm/dg15/en/media/dataprot/studies/servint.htm

[3] Ainsi appelé non parce qu'il se compose de 29 membres mais bien parce qu'il a été créé par l'article 29 de la Directive 95/46 du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des individus à l'égard du traitement de données personnelles et à la libre circulation de ces données. JOCE, 23 nov. 1995 No L. 281 p. 31. Ce groupe est composé de représentants des différentes commissions nationales de protection de données de l'Union européenne.

[4] Ces mécanismes ont été décrits en détails en juillet 1998 dans mon article "les traitements invisibles sur Internet" : http://www.droit.fundp.ac.be/crid/eclip/luxembourg.html présenté lors de l'école d'été de juillet 1998 à l'Université du Luxembourg.

[5] Le groupe 29 a récemment émis *une recommandation sur les traitements invisibles et automatiques sur Internet effectués par hardware et par software*. Cette recommandation est la première adressée non plus à ceux qui gèrent les données mais à l'industrie qui conçoit et distribue le hardware et le software qui permet de traiter ces données. Il apparaît en effet que ces produits, par conception, permettent des "traitements

fichés dans une gigantesque base de données comportementale située sur le territoire américain. Cette base contient pour chaque internaute individualisé son adresse IP (révélatrice de son fournisseur d'accès et donc de la société qui l'emploie) ; le type, la version et la langue du système d'exploitation et du browser utilisé ; certaines données navigationnelles (pages visitées, date et heure de la visite (permet de distinguer le professionnel du particulier)) ; les bannières publicitaires qui lui ont été soumises et, dans certains cas, sa réactivité par rapport à ces bannières ; enfin et surtout, les mots-clés tapés depuis plusieurs années sur certains moteurs de recherche[6].

Plus concrètement, cette possibilité de profilage à outrance est rendue techniquement possible par la combinaison de trois caractéristiques qui - prises individuellement – restent relativement inoffensives.

Les hyperliens invisibles

La notion d'hyperlien n'a plus à être détaillée. Elle constitue un élément essentiel de la navigation sur Internet. Toutefois, aux hyperliens explicites et visibles qui nécessitent une action objective de l'internaute pour voyager dans le cyberespace, s'opposent les hyperliens implicites et invisibles, s'exécutant sans intervention de l'utilisateur et à son insu. Ces hyperliens invisibles permettent d'inclure dans une page Web des images *issues d'autres sites*. Cette possibilité technique est largement utilisée pour la diffusion de bannières publicitaires stockées sur un seul site du réseau mais rendues visibles sur des milliers d'autres pages d'autres serveurs disséminés à travers le monde entier. Cette caractéristique, prise isolément, ne nuit pas à la protection de la vie privée de l'internaute.

Le bavardage des programmes de navigation.

Le " bavardage " des programmes de navigation constitue une deuxième caractéristique apparaissant comme d'avantage privacide[7]. Lorsqu'un programme de navigation demande une page à un site Internet, il communique de manière cachée et systématique certaines informations relatives à la machine du demandeur et notamment :

- Le type de système d'exploitation de la machine (Windows 95 ou 98, Macintosh ou Unix)
- Le type et la langue du programme de navigation (p.e. Netscape Navigator 3.01 Gold FR)
- Le type de processeur (Intel, Mac ou PowerMac,…)
- La langue parlée par l'internaute (p.e. le Français de Belgique)
- La page référente. Dans le cas d'un hyperlien classique, il s'agit donc de la page visitée avant la page précédente (en fait la page ou se trouvait l'hyperlien menant à la page actuelle). Dans le cas d'un hyperlien invisible, il s'agit de la référence de la page ou sera affichée la bannière publicitaire. Dans le cas d'une page fournissant les résultats d'une recherche, le nom de la page référente contient les critères de recherche (les mots-clés). En d'autres termes, un site de cybermarketing qui transmet une bannière destinée à être affichée dans les résultats d'un moteur de recherche sait, **avant de transmettre la bannière**, ce que l'utilisateur recherche. Il va de soit que ce site transmettra alors une bannière ad hoc au consommateur.

Cette deuxième caractéristique, associée à la première permet à des sociétés invisibles du réseau et inconnues du grand public de capter en temps réel le comportement de dizaines de millions d'internautes[8]. Toutefois, cette possibilité reste éphémère car l'internaute ne communique aucun élément qui l'identifie de manière stable. Il communique certes son adresse TCP/IP[9] mais cette adresse est attribuée dynamiquement par le fournisseur d'accès lors d'une connexion par modem. Il s'ensuit que cette adresse n'est pas un identifiant stable de l'utilisateur résidentiel.

---

invisibles" qui profitent principalement aux marchands et aux cybermarketeurs mais qui sont déloyaux par rapport au consommateur et contraires - si pas à la lettre, - en tout cas à l'esprit de la directive 95/46 précitée.

6 S. Gauthronet, op. cit., p. 92. Suivant un test effectué en 1998, ces informations sont liées à un cookie stocké en général à l'insu de l'utilisateur sur son propre PC et programmé pour persister jusqu'en l'an… 2030.

7 A comprendre comme liberticide ou insecticide : tueur de vie privée. Nous osons ce mot car il permet de conserver toute la force du " privacy killing " anglais.

8 Selon Gautronet (op. cit., p. 92) cite le chiffre de 17.000.000 pour une seule entreprise américaine.

9 Sur Internet, chaque machine est identifiée par un numéro unique composé de quatre nombres séparés par des points et allant de 1 à 255. On les note donc A.B.C.D. L'espace des adresses possibles fournit un potentiel théorique de plus de quatre milliard de machines connectées simultanément.

Les cookies

Les cookies sont constitués des informations qu'un ordinateur serveur (accédé par un hyperlien classique *ou invisible*) peut stocker, lire ou effacer de manière permanente sur le disque dur de l'internaute, généralement[10] à l'insu de celui-ci. Il s'agit en fait d'un code barre souvent inintelligible que n'importe quel site peut coller, supprimer ou modifier sur le dos de ses visiteurs, éventuellement par hyperlien invisible interposé.

L'avantage principal du cookie est qu'il est stable dans le temps et lié à une machine particulière. Il permet donc de s'affranchir du caractère dynamique de l'adresse TCP/IP de l'utilisateur résidentiel et de profiler une machine unique pour plusieurs dizaines d'années[11]. En d'autres termes, si un ordinateur aujourd'hui doté d'une adresse TCP/IP A.B.C.D. a reçu un cookie d'un site particulier (typiquement d'une entreprise de cybermarketing par hyperlien invisible), le même ordinateur transmettra systématiquement ce code barre à son insu à ce site (typiquement lors du téléchargement d'une bannière par hyperlien invisible) même s'il possède demain une adresse TCP/IP E.F.G.D ou R.T.U.V.

L'inversion du paradigme client-serveur

Ces trois caractéristiques *privacides* sont donc combinées pour produire un cocktail explosif redoutable permettant de traquer les actions-clés de chaque utilisateur. Par ailleurs ces utilisations habiles et sournoises de la technologie Internet provoquent un événement social déterminant que nous appelons l'inversion du paradigme client-serveur.

Le modèle client-serveur a longtemps été la base régissant les banques de données : un ordinateur serveur possède l'information qu'il délivre à un ordinateur client. Il s'agit d'une "relation" maître-esclave, postulant la docilité du serveur et la stabilité de l'information. Dans ce monde il n'y a pas, dans le chef de l'ordinateur serveur de discrimination. Chaque client, quel qu'il soit, effectuant une requête identique reçoit la même réponse. L'information n'est pas altérée. Ce modèle de consultation n'est pas très différent de ce qui se passe lorsqu'un lecteur se rend dans une bibliothèque afin de trouver et de consulter certains ouvrages. Pour effectuer l'interface entre une machine serveur située quelque part sur le réseau et un utilisateur humain, l'ingénierie logicielle a mis au point à un niveau planétaire un ensemble de protocoles répartis en plusieurs couches. Cette manière de procéder permet de maîtriser la complexité du processus de communication en hiérarchisant la programmation en couche, chaque couche ayant un rôle particulier à jouer. Plus concrètement, chaque couche se compose d'une série impressionnante de plusieurs centaines de sous-programmes informatiques réalisant certaines fonctions à l'intérieur d'une couche particulière. Ces sous-programmes sont exécutés d'une manière invisible pour l'utilisateur moyen. En fait chaque couche et les programmes qui s'y exécutent possèdent un degré historiquement croissant :

- d'indépendance par rapport à l'utilisateur (et bien souvent le propriétaire) de la machine : les programmes exécutent certaines actions que l'utilisateur n'a pas demandé,
- d'opacité par rapport à l'utilisateur : non seulement les centaines de sous-programmes effectuent des actions non demandés par l'utilisateur, mais l'utilisateur n'en est pas informé et n'a pas de moyens fiables de savoir ce qui se passe,
- de dépendance ou d'asservissement par rapport au réseau, ou plus précisément par rapport aux machines installées sur le réseau et censées délivrer passivement l'information. Ces machines peuvent envoyer des requêtes aux machines clients du réseau en vue d'obtenir certains renseignements sur l'utilisateur,

---

[10] Les utilisateurs avertis peuvent paramètrer leur navigateur de manière à inhiber les cookies ou à accepter au cas par cas mais ces mesures restent largement inappropriées parce que

1. L'utilisateur moyen ignore ce qu'est un cookie et quel sont ses risques en matière de vie privée
2. Certains sites refusent les visiteurs qui refusent les cookies
3. Certains sites envoient plusieurs cookies et provoquent harcèlement et fatigue chez l'internaute
4. Les mécanismes d'opposition empêchent la réception de nouveaux cookies mais non l'envoi des cookies précédemment reçus et enregistrées.
5. Etc.

[11] Il n'est pas rare que les entreprises de cybermarketing envoient des cookies conçus pour durer jusqu'en l'an 2035…ou plus.

- de transparence par rapport au réseau. Le réseau peut obtenir des informations précieuses sur le "naviguant[12]".

La comparaison entre Internet et une tera[13] bibliothèque - bien que probablement encore fort présente dans l'imaginaire social- ne tient plus la route. La technologie installée sur le PC de l'internaute obéit aujourd'hui autant à des *ordres étranges venus d'ailleurs* qu'à l'internaute lui-même.

Au delà des règles techniques bien souvent hermétiques et inconnues du grand public, un élément social fondamental est atteint. Profondément. Depuis que le livre est livre, l'information a toujours été "passive", chaque mot imprimé une fois pour toute, éventuellement reproduit dans un index, attendant patiemment parfois pendant très longtemps le regard d'un lecteur hypothétique. Depuis que le livre est livre, on n'a jamais vu un bouquin jaillir d'un rayonnage et s'ouvrir spontanément à une de ses pages pour attirer l'attention d'un lecteur. Depuis que les bibliothèques existent, on n'a jamais vu un ouvrage s'automutiler, s'arrachant certaines pages et s'en greffant d'autres selon le type de lecteur qui l'approcherait.

La technologie Internet, telle qu'actuellement implémentée permet un profilage précis, automatique et systématique de chaque internaute en particulier et, partant, un polymorphisme en temps réel de l'information qui lui est " soumise ". Le profilage permet à ceux qui détiennent l'information de filtrer, de trier, de cacher ou d'altérer l'information qu'ils possèdent avant de la communiquer. L'utilisation pernicieuse et invisible des technologies d'Internet permet de laisser l'illusion à l'internaute que l'information " délivrée " reste objective.

L'émergence d'une prise de conscience chez les utilisateurs

Si le profilage transcontinental des internautes européens, pratiqué sur une grande échelle par les entreprises américaines de cybermarketing se déroule jour après jour sans grande réaction de la part des organes européens chargés de l'application de la loi, d'autres événements allant dans le même sens ont provoqué de sérieux remous.

En janvier 1999, la décision rendue publique par Intel d'incorporer dans sa nouvelle gamme de processeurs un numéro d'identification unique accessible par le réseau a soulevé un tollé au USA et plusieurs organisations américaines ont publiquement appelé au boycott des nouveaux processeurs Intel[14].

En mars 1999, le quotidien libération[15] a rendu publique une pratique de Microsoft qui consistait à collecter une empreinte numérique[16] de l'ordinateur lors de l'enregistrement d'un utilisateur par Internet, même si ce dernier s'y opposait.

Au delà de la condamnation judiciaire de telles pratiques, l'émergence de cette prise de conscience est particulièrement encourageante et coïncide avec l'apparition d'une méfiance tardive mais légitime de l'internaute par rapport au réseau Internet.

---

[12] c'est à dessein que nous emploierons ce terme pour le différencier du terme navigateur qui désigne le programme utilisé par le naviguant.

[13] le dernier de la série : kilo, méga, giga, tera ; soit un billion.

[14] Voyez le site http://www.bigbrotherinside.com. Intel a toujours prétendu que l'identification ne pourrait se passer à l'insu de l'internaute. Une revue allemande a récemment prétendu qu'un expert en processeur avait trouvé une faille permettant d'activer ce Processor Serial Number à l'insu de l'internaute. (http://www.heise.de/ct/english/99/05/news1/)

[15] Laurent Mauriac, " *Un mouchard au cœur de Windows 1998. Microsoft accusé d'espionner ses clients ",* Libération du 8 mars 1999. (http://www.liberation.fr/multi/actu/semaine990308/art990309a.html) (Attention en allant voir cette page, vos données seront transmises à une société de cybermarketing…)

[16] Cette empreinte est plus fiable qu'un cookie et se baserait sur la combinatoire d'éléments matériels présents dans l'ordinateur. Pour la petite histoire et toujours selon Libération, Microsoft parle de " bug " (sic) mais aurait déclaré être prêt à supprimer de sa base les noms des utilisateurs qui ne veulent pas y figurer. Résumons. Le " géant du logiciel " constitue donc *malgré lui* une méga banque de données de ses utilisateurs en violant le devoir d'information garanti par la directive 95/46 mais en guise de dédommagement prévoit de fournir à *ceux qui le demandent* (=>seront-ils fichés ?) dans trois mois le droit d'opposition garanti depuis octobre de l'année passée par la dite directive. Et nous n'abordons même pas de la question de la légitimité de cette collecte d'information.

Technologie et contre technologie

Si les gens raisonnables s'accordent sur la nécessité de résoudre les problèmes générés par Internet et plus particulièrement le problème de la vie privée sur le réseau[17], les approches pour ce faire diffèrent en substance.

Une première approche consiste à concevoir une nouvelle technologie de manière à pallier aux déficiences de la première. Mais cette approche suppose que la technologie elle-même est capable de juguler les perturbations non techniques qu'elle engendre. Métaphoriquement on pourrait dire que la conception de pots d'échappements catalytiques est la solution technique proposée pour résoudre le problème social et médical de la pollution atmosphérique issue des moteurs à explosions. Actuellement, le protocole P3P[18] est représentatif de cette tendance. L'idée de base de P3P est la suivante : l'utilisateur confie à son programme de navigation ses données personnelles ainsi que les finalités pour lesquelles ces données peuvent être communiquées à des tiers. Lors d'une connexion avec un site, un dialogue invisible[19] s'établit entre le site et l'internaute ; le site déclare ses pratiques et les finalités pour lesquelles il souhaite utiliser les différents types de données. S'il y a accord entre les *privacy preferences* de l'utilisateur et les *privacy practices* du site, les données seront transférées. Dans le cas contraire, les données ne seront pas transférées et une négociation pourrait avoir lieu[20, 21].

Ce protocole a toutefois suscité une réaction de la part du Groupe de travail 29[22] qui a souligné que *" qu'une plate-forme technique pour la protection des données ne sera pas en elle-même suffisante pour protéger la vie privée sur Internet "* et que " *P3P peut induire en erreur les opérateurs basés en Europe en leur faisant croire qu'ils peuvent être déchargés de certaines de leurs obligations (p.e. garantir le droit d'accès) si l'utilisateur [de P3P] y consent "*. La protection de la vie privée relève en effet de l'ordre public et l'utilisateur, même consentant ne peut renoncer de manière définitive aux droits fondamentaux que la loi lui octroie. Ceci n'exclut pas qu'il puisse monnayer l'usage ou la communication de ses données contre des avantages divers, mais il serait contraire à l'ordre public de le voir renoncer, même de manière volontaire, à exercer son droit d'accès.

Il faut souligner des côtés plus pernicieux du protocole P3P tel que conçu actuellement.

- Il suppose implicitement que la solution à la protection des données est la déclaration des pratiques en matière de vie privée par le site. Cela suppose une honnêteté absolue de la part de tous les sites dans un contexte où aucune sanction n'est envisagée.
- Il déplace la charge de la protection des épaules du responsable du traitement sur les épaule de la personne concernée. Il ne s'agit plus d'acheter une voiture avec un pot d'échappement catalytique mais un masque à gaz car toutes les voitures seront livrées d'origine sans système de dépollution. Celui qui veut se protéger n'a qu'a être malin et… payer. La directive garantit le droit à la vie privée pour tous, même pour les simples d'esprit et les pauvres et ce même malgré eux.

---

17 Durant ces dernières années, le droit à l'anonymat sur le réseau a été affirmé par la conférence de Bonn, l'OCDE, le groupe 29, le groupe de Berlin, etc. Encore faut-il s'entendre sur le terme anonymat. La restriction aux seules caractéristiques de l'identité civile me semble ringarde eu égard aux méthodes ***d'identification anonyme*** actuellement effectives sur Internet. Le patronyme n'est qu'un aspect peu pertinent de l'identité dans le monde virtuel. A ce sujet lire Jean-Marc Dinant, " L'électronisation du commerce ", à paraître dans la *Revue Générale* du mois de mars 1999.

18 P3P est l'abréviation de Platform for Privacy Preferences. Il s'agit d'une norme en cours d'élaboration par le W3C. Les spécifications techniques de ce protocole sont disponibles sur le site du World Wide Web Consortium : http://www.w3c.org/P3P

19 Il se situe au niveau de l'entête HTTP et donc, contrairement à PICS par exemple, hors du HTML. L'entête HTTP est le lieu technique où sont transmis les fameux cookies et le dialogue reste donc invisible (" seamless ") par un utilisateur même averti.

20 L'idée de négocier ses données contre des avantages peut paraître choquante aux défenseurs de la privacy. Toutefois, cette situation reste un progrès par rapport à la situation actuelle où des sociétés invisibles captent ces données à l'insu de l'utilisateur et sans contrepartie.

21 "*Designing a Social Protocol : Lessons Learned from the Platform for Privacy Preferences*.", Lorrie Faith Cranor, Joseph Reagle Jr., Alexandria, VA, septembre 1997. http://www.research.att.com/~lorrie/pubs/dsp/dsp.html.

22 Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS) : http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp11fr.pdf.

- Il oublie que les préférences en matière de vie privée constituent des données à caractère personnel et qu'il faut à tout prix éviter que les personnes soucieuses de préserver leur anonymat se retrouvent elles-mêmes fichées pour cette seule raison.
- Il repose sur un moteur de confiance (trust engine) qui va veiller sur les données personnelles. Un système qui demande des données personnelles afin de les garder peut-il raisonnablement être considéré comme plus fiable qu'un système qui ne les possède pas ? (comme c'est le cas actuellement)
- P3P ne propose pas une solution globale aux autres problèmes de protection des données sur Internet comme les cookies, les empreintes numériques crées par Microsoft ou le numéro d'identification des processeurs Intel PIII.

En conclusion, s'agissant d'une contre technologie, P3P dans le stade actuel n'offre pas une solution globale aux attaques de différents types pouvant survenir sur le réseau mais une solution partielle reposant sur un code de conduite invisible de l'internaute. En outre, il modifie de manière insidieuse l'esprit même de la directive 95/46 dans la mesure où c'est l'internaute lui-même qui doit remplir un formulaire de déclaration des ses pratiques en matière de vie privée alors que les articles 18 et 19 de la directive précitée font clairement peser cette obligation sur les épaules du responsable du traitement.

La cryptographie comme réponse aux atteintes à la vie privée.

Bien souvent, principalement sur les sites américains[23], la cryptographie est présentée comme l'outil absolu et souverain de protection des données. Toutefois, la cryptographie[24] est souvent envisagée dans le seul contexte du courrier électronique. Même dans ce cadre, son usage reste limité car, en général, seul le contenu des messages est chiffré et les adresses électroniques des destinateurs et destinataires circulent donc en clair sur le réseau.

Il existe une panoplie impressionnante d'outils de cryptage sur Internet. Le problème majeur réside dans le niveau de compétence nécessaire pour permettre à un individu de choisir un bon algorithme de chiffrement. Le monde des cryptographes est un jeu de gendarmes et de voleurs et de nombreux algorithmes considérés comme sûrs hier sont " cassés " en quelques jours aujourd'hui. L'exemple le plus marquant est le DES 56 bits[25] qui n'a résisté que 22 heures aux attaques conjuguées de deux organisations américaines (distributed.net et l'Electronic Frontier Fundation)[26]. En Juillet 1998, le DES 56 bits avait déjà été cassé par l'EFF en 56 heures. Il est intéressant de constater que ces deux organisations utilisent des méthodes différentes pour aboutir à des puissances de déchiffrement imposantes. L'EFF a produit un super ordinateur spécialement conçu pour casser des clés. Distributed.net[27] utilise le temps mort (idle time) de plusieurs dizaines de milliers d'ordinateurs personnels connectés au réseau, chacun tentant de casser un petit nombre de clés. Ceci ne crée aucun ralentissement de la machine connectée, le programme de déchiffrement tournant en tâche de fond, lorsque l'ordinateur client ne fait rien.

Ceci est préoccupant lorsque l'on sait que le DES 56 est le protocole conseillé par le gouvernement américain pour protéger les informations non militaires. Mutatis mutandis, il conviendrait de pouvoir ramener cette insécurité du chiffrement du DES 56 bit au protocole SSL qui est le standard de chiffrement utilisé par les navigateurs courants. Ce protocole permet classiquement, outre un chiffrement (typiquement lors de l'envoi de numéros de cartes de crédit), l'identification du site visité (techniquement parlant par le biais d'un tiers de confiance). Ce protocole fonctionne avec une clé de quarante bits dont le nombre de possibilité est 2 puissance 16 fois inférieur au DES 56 bits. Elle est donc cassable en 65.536 fois moins de temps. Tous calculs faits, une personne décidée à investir deux millions de FB pour construire un ordinateur semblable à celui de l'EFF pourrait théoriquement casser dix millions de clés 40 bits par année dans un délai moyen de 3 seconde par clé et pour un coût moyen par clé cassée de l'ordre de quelques centimes. Ce délai est très court et permettrait à un tiers d'intervenir dans la communication.

---

23 Voyez notamment : http://www.epic.org/ ; http://www.cdt.org/ ;

24 " L'art et la science de garder le secret des messages " selon Bruce Schneier in " Cryptographie appliquée ", Internatinal Thomson Publishing France, Paris, 1997, p. 1.

25 Data Encryption System. 56 bits est le nombre de bits de la clé. En général plus la clé est longue, plus elle s'avère difficile à casser.

26 http://www.eff.org/pub/Privacy/Crypto_misc/DESCracker/HTML/19990119_deschallenge3.html

27 http://www.distributed.net

En conclusion, la cryptographie pourrait constituer une base fiable garantissant un certain degré de confidentialité (le contenu des messages) à condition d'utiliser des clés de longueur " suffisante " et des algorithmes dûment testés. Toutefois, si cette solution peut procurer une solution dans le cadre du courrier électronique, elle demeure peu utilisée et faible au niveau téhorique comme précaution contre le spamming[28] ou les traitements invisibles.

Privacy Enhanced Technologies.

Il s'agit ici d'introduire un nouveau concept par un jeu de mots (Privacy Enhancing Technologies => Privacy EnhanceD technologies). L'idée sous-jacente n'a rien d'original[29] mais consiste à implémenter, au niveau industriel lui-même, dans la conception des logiciels et du matériel des mécanismes protecteurs des données[30], ou plus exactement entre deux implémentations de protocoles techniques, choisir la moins privacide.

Il est extrêmement édifiant de constater que dans la norme technique HTTP 1.1[31]., le mot " privacy " intervient une vingtaine de fois. Par contre, lors de l'implémentation de ce protocole, l'industrie informatique n'a pas tenu compte de ces considérations. En fait, si la normalisation est constituée d'un ensemble de règles destinées à assurer l'interopérabilité au niveau mondial, elle laisse néanmoins une certaine marge de manœuvre lors de l'implémentation. Très concrètement, si le contenu obligatoire des entêtes HTTP 1.1 est réglementé strictement, l'ajout de cookies ou d'autres éléments de bavardage dans ces entêtes n'empêche pas l'interopérabilité entre le site Internet et son visiteur.

Depuis qu'Internet a été investi par les marchands[32,33], l'implémentation des protocoles par *ceux qui savent* permet d'inverser ce rapport client/serveur. Le client devient subrepticement le serveur des informations personnelles de l'internaute au service du réseau. L'internaute ne possède plus aujourd'hui aucun droit de regard effectif et techniquement efficace sur les données que son programme envoie malgré lui sur le réseau. Il nous semble évident que les procédés actuellement répandus seraient inacceptables et inacceptés dans le monde réel : pourrait-on imaginer que chaque commerçant commence à filmer tous les faits et gestes (achats, non achats, regards, habillement, langue, type et âge de la voiture…ou du vélo, compagnie, etc…) de chacun de ses clients et colle un code barre identifiant dans le dos de chaque client pour partager ces données avec ses copains dans le monde entier ?

Sur Internet, cela est aujourd'hui possible et largement réalisé. Un bon usage des PETS peut être de dénoncer ces pratiques afin de ficher les mauvais ficheurs afin que les technologies privacides s'adaptent aux exigences des internautes scandalisés. Il est illusoire d'espérer des " autoroutes " de l'information respectueuses de la vie privée tant que les véhicules y circulant resteront des pompes à données personnelles conçues par une industrie financée par les marchands. Bien plus que le consommateur, c'est au citoyen lui-même qu'il appartient de s'éduquer et d'appliquer le " drag and drop " aux technologies liberticides. Sur ce terrain et contrairement aux idées reçues, les américains ne sont pas nécessairement moins bien embarqués que les européens. Peut-être les organisations de consommateurs américaines appelant au boycott d'Intel obtiendront-elles, - en l'absence de toute législation impérative -, un résultat tangible et rapide.

---

[28] Le courrier électronique sauvage. Certaines firmes (heureusement minoritaires) envoient des publicités à un nombre maximum d'internautes.

[29] L'insertion de mécanismes de dépollution et de réduction de consommation est effective depuis plus d'une dizaine d'années au sein de l'industrie automobile qui reste florissante. Toutefois une condition sine qua non est que tous les constructeurs soient soumis aux mêmes exigences. Dans le cas contraire, des contraintes différentes en matières de respect de la vie privée pourraient causer une distorsion de la concurrence.

[30] Cette idée est la base d'une récente recommandation du Groupe 29 : http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp17en.pdf

[31] HyperText Transfert Protocol constitue le protocole utilisé pour *surfer sur le web*

[32] Netscape Navigator et Internet Explorer sont donnés gratuitement depuis peu. Les programmes clients sont offerts mais les programmes serveurs sont vendus (NT Server ou Netscape Commerce Server p.e.) aux entreprises. Les entreprises paient pour une technologie client/serveur qui permette une connaissance intime de leurs clients.

[33] Voir Dan Schiller ,"Les marchands à l'assaut d'Internet " in Le Monde Diplomatique n°516, Paris, mars 1997

L'obstacle principal reste le faiblesse des connaissances techniques de l'internaute moyens…et des webmestres[34] eux-mêmes. Ainsi, un journal de petites annonces établis à Bruxelles n'accepte pas la visite des internautes refusant les cookies (non rémanents il est vrai). Il y a peu, le site www.ready.be publiait très probablement en toute bonne foi dans ses " questions souvent posées " qu'il n'utilisait pas de cookies rémanents, ce qui était faux. En fait, il envoyait un cookie expirant en l'an 2009[35]. Il apparaît que ces deux sites utilisent tous deux un serveur Microsoft. La technologie serait-elle aussi opaque pour les entreprises qui l'utilisent en payant que pour les internautes qui la subissent gratuitement?

---

[34] Terme français exact pour désigner les techniciens qui gèrent un site Internet (Webmaster en anglais). A comprendre par analogie avec le bourgmestre.

[35] Ceci repose sur une expérimentation personnelle effectuée le 15 février 1999 dans l'après-midi.